REMARKS

Reconsideration of the instant application is respectfully requested. The present submission is responsive to the Office Action of September 7, 2005, in which claims 1-24 are presently pending. A courtesy copy of the claims in their present form is included above. With regard to the art of record, and following the disqualification of U.S. Patent Publication 2002/0144108 to Benantar as a prior art reference under 35 U.S.C. §103(c), each of claims 1-24 now stands rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent 6,671,804 to Kent, in view of U.S. Patent Publication 2005/0114666 to Sudia. For the following reasons, however, it is respectfully submitted that the application is in condition for allowance.

For an obviousness rejection to be proper, the Examiner must meet the burden of establishing that (1) all elements of the claimed invention are disclosed in the prior art; (2) that the prior art relied upon, coupled with knowledge generally available in the art at the time of the invention, must contain some suggestion or incentive that would have motivated the skilled artisan to modify a reference or to combine references; and (3) that the proposed modification of the prior art must have had a reasonable expectation of success, determined from the vantage point of the skilled artisan at the time the invention was made. *In re Fine*, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988); *In Re Wilson*, 165 U.S.P.Q. 494, 496 (C.C.P.A. 1970); *Amgen v. Chugai Pharmaceuticals Co.*, 927 U.S.P.Q.2d, 1016, 1023 (Fed. Cir. 1996).

Thus, under the first element, to establish *prima facie* obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). If an independent claim is

nonobvious under 35 U.S.C. §103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

In the present Office Action (page 3), the Examiner acknowledges that Kent is silent with regard to constructing the proof of possession confirmation in a manner so as to prevent replay attacks by an impostor. Thus, the Examiner further cites Sudia (in combination with Kent) in support of the present §103 rejections by indicating that Sudia discloses an "authentication method for requesting an attribute certificate that comprises multiple fields, and a hash string, which is utilized to authenticate and proof of possessing the certificate... Therefore, it would have been obvious at the time of the invention for one having ordinary skill in the art to modify Kent's invention to incorporate hash string of information as a key to encrypt the requesting object with the motivation of strengthening the authentication security."

However, a review of the Sudia reference reveals that it does not in fact provide the capability of preventing replay attacks by an impostor. First, Sudia does not actually teach incorporating a hash string of information as a key to encrypt the requesting object, as stated by the Examiner. Rather, the Sudia reference deals with holding information locally and including a hash (e.g., the root node of a hash tree) in a certificate or request to prove that the information has not been changed if the certifier is subsequently challenged. (See Sudia, Abstract) For example, in paragraph [0242], Sudia teaches calculating a blocker key value as an encryption (using a pre-shared key) of the hash of various information in the attribute certificate.

Second, even if the incorporation of hash string information as an encryption key were taught in Sudia, this would not accomplish the purpose of preventing replay attacks, since one skilled in the art would realize that anyone having access to the certificate request itself could also calculate the hash string. In other words, using a hash string as an encryption key is useless for the purpose of preventing replay attacks. In contrast, claim 3, for example, of the instant application recites that the key identifier is extracted

from the (encrypted) proof of possession structure. That is, the key identifier is not used as the encryption mechanism itself (where it could be determined by anybody with access to the request), but is instead a part of the encrypted POP structure.

Therefore, because the claimed element of constructing the proof of possession confirmation in a manner so as to preventing replay attacks by an impostor is not taught in either Kent or Sudia, the claims are not anticipated by a combination of the two references. The Applicants therefore respectfully traverse the §103 rejections of claims 1-24, and respectfully request reconsideration and withdrawal of the same.

For the above stated reasons, it is respectfully submitted that the present application is now in condition for allowance. No new matter has been entered and no additional fees are believed to be required. However, if any fees are due with respect to this Amendment, please charge them to Deposit Account No. 09-0463 maintained by Applicants' attorneys.

Respectfully submitted,
THOMAS L. GINDIN, ET AL.

CANTOR COLBURN LLP
Applicants' Attorneys

By _____
Sean F. Sullivan
Registration No. 38,328
Customer No. 46429

Date: December 7, 2005
Address: 55 Griffin Road South, Bloomfield, CT 06002
Telephone: (860) 286-2929